INFORMATION SECURITY REQUIREMENTS

Litera requires that third party vendors, consultants, developers, subcontractors, agents, and other third parties and non-Litera employees ("Vendor/s") take reasonable security measures to guard the confidentiality, integrity, and availability of Litera Information when shared or made accessible to them to fulfill the Purpose. The requirements cover, at a minimum, how Litera expects Vendors to use, store, transmit, dispose of, process, or otherwise handle Litera Information.

Purpose: Vendor provides goods, software, deliverables or services to Litera in accordance with the agreed specifications, timelines and quality standards. Litera Information: any data or information shared by Litera, whether prior to or following the commencement of the engagement to fulfill the Purpose; or data or information to which Vendor derives or gains access to while fulfilling the Purpose. Litera Information may include but is not limited to customer information or data, employee information or data, product information, trade secrets, financial data, or any personally identifiable data as identified by applicable privacy laws, outputs or results derived from Litera's use of Vendor's software or services or login information to Litera systems when Vendors are provided such access.

Litera expects the Vendor to stay informed of and in compliance with all applicable data security statutes, regulations, or other requirements in order to identify, protect, and secure Litera data.

To the extent Vendors have entered into an agreement with Vendors to fulfill the Purpose and in the event of conflict between such agreement and this Information Security Requirements, the latter shall prevail and govern.

I. Information Security Policy
   - A. The Vendor shall designate an Information Security Officer responsible for overseeing the implementation and maintenance of information security controls. Senior management shall demonstrate commitment to information security by approving policies, allocating resources, and reviewing security performance at least annually.
   - B. The information security policy must be periodically reviewed, updated, and approved by Vendor management.
   - C. The Vendor must communicate in writing information security requirements including their security roles and responsibilities, to all personnel working on Litera matters and enforce compliance.
   - D. The Vendor must establish and administer information security training to all employees at least annually.
   - E. The Vendor conduct formal risk assessments at least annually, or upon significant changes, to identify, evaluate, and treat risks to Litera Information. Risk assessment results and mitigation plans shall be documented and made available to Litera upon request.

II. Background Checks & Confidentiality
   - A. Background checks must be performed on all permanent and temporary employees who have access to Litera Information. The scope should include, at a minimum, criminal and financial checks, where permitted by law.
   - B. If screening has not occurred or adverse information is discovered, the Vendor shall provide notification to the Litera point of contact.

III. Physical Access Controls
   - A. The Vendor must implement reasonable access controls to offices, work areas, and computing rooms to limit the exposure of Litera Information to those with a need to access.
   - B. Litera Information must be stored within facilities located in the United States, unless otherwise authorized in writing by the Litera. Where Litera data is stored outside of the United States, the Litera expects that the Vendor has taken positive steps to comply with local data protection laws and will make those steps available to the Litera.

IV. Physical Document Security
   - A. The Vendor must implement reasonable physical protection around work papers and documents.
   - B. Where Litera information is provided in physical form, Litera information must be returned, deleted or destroyed, at Litera's discretion at the end of Litera's engagement or upon Litera's request or upon termination or expiration of the Vendors contractual terms with Litera.
   - C. Upon request, the Vendor will furnish a certificate that Litera Information has been securely deleted or destroyed.
   - D. The Vendor must reasonably protect against losses of Litera Information due to theft, fire, water or other environmental causes.

V. Third-Party Relationships
   - A. The Vendor must establish procedures to verify, including periodic assessments, that all third-party Vendors with access to Litera Information have policies and procedures equivalent to these Information Security Requirements.
   - B. If the Vendor proposes using a hosted or cloud environment to process or store Litera Information, Vendor must only use a U.S. based, privately hosted or dedicated cloud environment (e.g., Microsoft Azure, Amazon AWS) that encrypts the Litera Information while at rest.

VI. Access Controls
   - A. The Vendor shall enforce the principle of least privilege and conduct periodic reviews (at least quarterly) of user and system access rights to Litera Information. Formal processes for access requests, approvals, and removals shall be documented and followed.

B. The Vendor must have written processes and controls for managing network and user IDs, including the provisioning, changing, and disabling of accounts.
    1. User login accounts shall be automatically disabled when inactive for more than 90 days.
    2. User login accounts for terminated users shall be disabled within 24-hours.
C. All systems and computers must be protected with secure password management, including unique passwords that periodically expire, are a minimum password length of at least 12 characters and complexity (special characters or numbers), lock out after limited number of failed attempts, and limit reuse.
D. Users must be prohibited from storing, sharing, or writing down passwords.
E. The Vendor must have written processes to control and limit access to system and administrative accounts.
F. The Vendor must require the use of multifactor authentication when accessing Litera Information on Vendor's systems and/or Vendor's third-party systems.

VII. Computer and Device Security
A. Anti-virus/anti-malware software must be installed on computers and configured to identify and clean viruses/malware automatically while providing notification of the activity.
    1. Anti-virus/anti-malware software definitions must be updated in a timely manner.
B. The Vendor must apply security software updates and patches promptly following their release by applicable software publishers.
C. The Vendor must use 128-bit encryption or industry standard, (whichever is greater) on all laptops, mobile devices, and any other hardware, device or appliance that contains Litera Information.
D. The Vendor must configure mobile devices with reasonable protections, including device PINs, auto-locking timeouts, and remote wipe capabilities.
    1. When personal devices are used, they must be managed by a Vendor-controlled Mobile Device Management system that can enforce these security requirements and segregate Litera information from personal information.
E. Litera does not permit the use of removable media (e.g., CDs, DVDs, USB thumb drive, memory cards) for Litera Information unless it is encrypted using an industry standard algorithm of 256-bits strength or more.
F. The Vendor must establish procedures to securely erase or destroy Litera Information stored in all databases, and on all laptops, mobile devices, and electronic removable media prior to offsite maintenance, recycling, resale, reassignment, or disposal.
G. Upon request, Vendor will furnish documentation that Litera Information has been securely destroyed where documentation may be satisfied in form of an email.

VIII. Infrastructure and Network Controls
A. Vendor must appropriately segregate computer networks using industry standard controls (e.g., firewalls) that prevent unauthorized access to systems containing Litera Information.
    1. Further, the Vendor must segregate Litera Information from other records, including when stored on backup media.
B. The Vendor must implement and maintain controls to secure and limit remote access to Vendor's systems and applications that store Litera Information.
C. Wireless access points that provide access to Vendor systems must be configured to only permit authorized devices and users to connect using no less than WPA2 encryption.
D. The Vendor must have established procedures for detecting, remediating and, where appropriate, reporting unauthorized or excessive access, copying, or misuse of Litera Information.
E. The Vendor must maintain logs of electronic access to systems containing Litera Information for at least one year and as otherwise required by law.

IX. Use of Information
A. The Vendor is responsible for the appropriate use of Litera Information. Litera Information must not be processed or otherwise used for any purpose other than explicitly stated in the contract between Litera and Vendor. Where this is not explicitly stated the Vendor must seek clarification from Litera regarding proper use.
B. The Vendor must not use Litera information in non-production environments (e.g. development or test environment) without express written authorization by Litera.

X. Electronic Communications
A. The Vendor shall maintain a documented cryptography policy covering the use, management, and protection of cryptographic keys. All cryptographic controls shall be reviewed annually for effectiveness and compliance with industry standards.
B. The Vendor is responsible for maintaining confidential communications pursuant to its duties to preserve confidentiality and to competently safeguard information relating to Litera.
C. The Vendor must use Litera's share site (secure.litera.com) or other encrypted methods to send, transmit, or transfer any Litera confidential, trade secret, or Personal Information.

XI. Business Continuity/ Disaster Recovery

A. The Vendor must establish and maintain business continuity and disaster recovery plans with comprehensive recovery strategies to address business interruptions that would disrupt services provided to Litera.

B. The Vendor shall test business continuity and disaster recovery plans at least annually, document test results, and update plans as necessary. Evidence of testing and plan updates shall be provided to Litera upon request.

C. Upon request, the Vendor will provide evidence of an executive summary of Business Continuity/Disaster Recovery Plan to Litera where such evidence shall be satisfied in the form of a summary.

XII. Travel Security

A. The Vendor must properly secure hard-copy documents, storage devices, and/or laptops to avoid theft while traveling.

B. The Vendor must exercise due care to avoid disclosure when discussing Litera matters and information in public areas or in transit.

C. The Vendor must utilize a Vendor-authorized VPN while working remotely or when connecting to public wireless networks.

D. The Vendor must not take Litera Information outside of the United States without prior written approval from the Litera.

XIII. Incident Management and Breach Notification

A. The Vendor must establish and maintain a documented plan and associated procedures for managing an information security incident, including documented routine exercise of the plan.

B. Upon request, the Vendor will provide evidence of an executive summary of such incident management and breach notification plan where such evidence shall be satisfied in the form of a summary.

C. Confirmed or suspected data breaches or security incidents that impact Litera Information must be reported, in writing, to appropriate Litera point of contact or legal@litera.com within twenty-four hours of such incidents/breach.

D. The Vendor should not notify any other parties of a data breach or security incident or compromise of Litera Information without prior written consent from Litera, other than as required by federal, state or other applicable law. Nothing precludes Vendor from notifying the data breach or security incident of other Customer's information so long as it does not notify the data incident or security incident of Litera Information.

E. In cases where further investigation is required, the Vendor agrees to work with Litera to provide notice of the proposed third-party incident response Vendor to allow for a conflict check.

XIV. Regulatory Compliance

A. The Vendor shall implement controls to ensure compliance with applicable data privacy laws and intellectual property protection requirements. The Vendor shall promptly notify Litera of any changes in legal or regulatory obligations affecting Litera Information.

B. Litera expects the Vendor to provide reasonable and necessary documentation in support of Litera's internal and external audits (e.g., HIPAA) upon Litera's request.

C. The Vendor must comply with all applicable requirements communicated by Litera for handling information/services concerning special handling. This includes applicable conditions imposed by government entities or other third-party restrictions on handling/access outside of the United States.

XV. Independent Third-Party Audits

A. The Vendor must periodically engage an independent third-party company to audit and test the Vendor's information security controls. A process must be established to resolve any risks or issues that are identified.

B. Upon request, the Vendor will provide evidence of an executive summary of such audit and test results and verify any identified deficiencies were remediated where such evidence shall be satisfied in the form of a summary.

XVI. Right to Audit

A. The Vendor shall make available to Litera all information necessary to demonstrate compliance with the Vendor's obligations under this Agreement and allow for and contribute to audits, including inspections during normal working hours, conducted by Litera or an auditor appointed by Litera that relate to the Vendor's compliance with its obligations under this Agreement.